Physical Facility Access Policy

Table of Contents

1. Overview

Management, technical staff, Admin and Support staff, Factory Operators, and security personnel are responsible for facility access requirements. The management and monitoring of physical access to facilities is extremely important to SFO security and helps maintain information as well as employee safety.

2. Purpose

This policy establishes rules for management, control, monitoring, and removal of physical access to SFO facilities.

3. Scope

This policy applies to all SFO staff.

4. Policy

A. General

Physical access to all restricted facilities shall be documented and managed. All facilities must be physically protected relative to the criticality or importance of the function or purpose of the area managed.

Requests for access shall come from the applicable manager in the area where the data/system resides. Access to facilities will be granted only to personnel whose job responsibilities require access. Electronic access control systems shall be used to manage access to controlled spaces and facilities.

The process for granting card and/or key access resides with the SFO IT Department. They shall regularly review card and/or key access rights and remove access for individuals that no longer require access or persons who leave SFO. Access rights shall be based on an employee's (staff, visitor, contractor, etc.) role or function in the organization.

B. Management Responsibilities

The IT Department or their designee shall ensure:

- Secure areas are protected by appropriate entry and controls for authorized personnel
- Procedures control and validate a staff member's access to facilities with the use of security personnel, identification badges, or electronic key cards
- Procedures exist that establish visitor controls including visitor sign-in logs and wearing of visitor badges for both entry and exit at SFO
- Policies specify management's review of the list of individuals with physical access to facilities containing sensitive information (whether in paper or electronic forms)
- A complete inventory of critical assets is maintained with SFO ownership defined and documented

- Card access records and visitor logs for facilities are kept for periodic review based upon the criticality of the information being protected and security necessity

- Access List and permissions are maintained and strictly enforced and changes are documented and logs kept updated.

C. KEY ACCESS AND CARD SYSTEMS

The following policy applies to all facility access cards/keys:

- Employee access cards and/or keys must not be shared or loaned to others

- Access cards/keys shall not have identifying information other than a return mail address and all cards/keys that are no longer required must be returned to SFO IT Department.

- Lost or stolen cards/or keys must be reported immediately to SFO IT Department.

- SFO IT Department shall remove card and/or key access rights of individuals that change roles or are separated from their relationship with SFO.

- The IT Security Manager or their designee regularly reviews access records and visitor logs for the facility and is responsible for investigating any unusual events or incidents related to physical facility access

D. VISITOR AND GUEST ACCESS

The following policy and procedure apply to identification and authorization of visitors and guests to SFO:

- Any SFO facility that allows access to visitors shall track visitor access with a sign in/out log

- A visitor log shall be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where sensitive information is stored or transmitted

- The visitor log shall document the visitor's name, the firm represented, and the on-site personnel authorizing physical access on the log

- The visitor log shall be retained for a minimum of three months, unless otherwise restricted by rule, regulation, statute, or SFO audit control

- Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel

- Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration

- Visitors shall be authorized before entering, and escorted at all times within, areas where sensitive information is processed or maintained

- Visitors must be escorted in card access controlled areas of facilities

E. CONFIDENTIAL AREA ACCESS

The following policy and procedure pertain to access to confidential SFO areas:

- All areas containing sensitive information shall be physically restricted
- All individuals in these areas must wear an identification badge on their person so that both the picture and information on the badge are clearly visible to SFO personnel
- Restricted IT areas such as data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing IT resources shall be restricted based upon functional business need
- Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted
- Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information
- Appropriate facility entry controls shall limit and monitor physical access to information systems
- Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas and this data shall be stored for at least 30 days, unless otherwise restricted by rule, regulation, statute, or law

IT Department staff shall:

- Implement physical and/or logical controls to restrict access to publicly accessible data ports (for example, data jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized)
- Ensure visitors are escorted at all times in areas with sensitive information
- Areas accessible to visitors should not have enabled data jacks unless network access is provided to a secure guest network only
- Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines
- Control physical and logical access to diagnostic and configuration ports
- Receive prior authorization before disposing, relocating, or transferring hardware, software, or data to any offsite premises

F. PHYSICAL SITE ACCESS

On-site physical access to sensitive or confidential areas for shall be controlled though a combination of the following mechanisms:

- Security based on individual job function

- Revocation of all facility access immediately upon termination and collection of keys, access/smart cards, and/or any other asset used to enter SFO facilities

Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization's premises.

G. CONTRACTOR REQUIREMENTS

External contractors shall comply with applicable laws and regulations regarding security and background checks when working in SFO facilities. For unclassified personnel, an appropriately cleared and technically knowledgeable staff member shall escort the individual to the area where facility maintenance is being performed and ensure that appropriate security procedures are followed.

- Any system access, initiation or termination shall be performed by the escort
- Keystroke monitoring shall be performed during access to the system
- Prior to maintenance, the information system is completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured
- Maintenance personnel must not have visual or electronic access to any sensitive or confidential information contained on the system they are servicing
- Devices that display or output sensitive information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information
- All personnel granted unescorted access to the physical area containing the information system shall have an appropriate security clearance

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of normal SFO operations. Examples of acceptable controls and procedures include:

- Visitor logs
- Access control procedures and processes
- Operational key-card access and premise control systems
- Operational video surveillance systems and demonstrated archival retrieval of data

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all SFO staff.

8. Policy Version History

Version	Date	Description	Approved By
1.0	05/07/2021	Initial Policy Drafted	